Published on *The National Law Review* https://www.natlawreview.com

High Alert: China Linked BlackTech Hides in Router Firmware

Article By:

Linn F. Freedman

Not only is the People's Republic of China (PRC) a threat with its use of TikTok, but it also supports threat actors that have for years attacked U.S. based companies as well as the governments of the U.S. and Japan. According to a Joint Advisory published on September 27, 2023, by the National Security Agency, the FBI, CISA, the Japan National Police Agency and the Japan National Center of Incident Readiness and Strategy for Cybersecurity, "BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships for pivoting from international subsidiaries to headquarters in Japan and the U.S.—the primary targets."

In addition to targeting entities that support the U.S. and Japanese governments and militaries, BlackTech has targeted "industrial, technology, media, electronics, and communications sectors." Its custom malware, dual-use tools, and living off the land tactics, such as disabling logging on routers, to conceal their operations."

The Advisory provides detailed detection and mitigation techniques for organizations and recommends "monitor[ing] network devices for unauthorized downloads of bootloaders and firmware images and reboots. Network defenders should also monitor for unusual

traffic destined to the router, including SSH.”

National Law Review, Volumess XIII, Number 271